PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-324219
(43)Date of publication of application : 08.11.2002

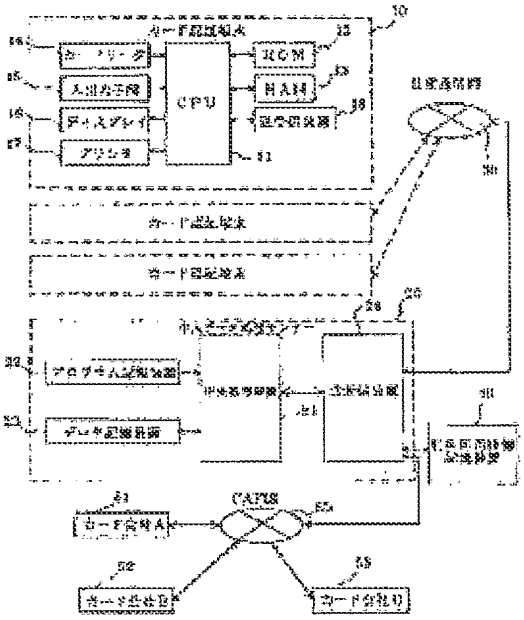
(51)Int.Cl. G06K 17/00
B42D 15/10
G06F 15/00

(21)Application number : 2001-126416
(22)Date of filing : 24.04.2001

(71)Applicant : SEIKO INSTRUMENTS INC
(72)Inventor : TACHIBANA HITOSHI

(54) CARD AUTHENTICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a card authentication system capable of preventing the illegal use of a card due to forgery on a high level.
SOLUTION: This card authentication system is provided with a plurality of card authenticating terminals 10 and a central data processing center 20 connected through a public communication network 30 to those card authenticating terminals so that on-line authentication processing can be executed by the card authenticating terminal 10 by performing access from the central data processing center 20 through a card business integral network system 50 to the respective host computers of card companies 51-53. This card authentication system is provided with a use validity/invalidity information storage device 40 for allowing each card user to preliminarily switch the validity/invalidity of the card, and the on-line authentication is executed only to the card whose use is judged to be valid through the use validity/invalidity storage device 40 by the central data processing center 20.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－324219
（P2002－324219A）
(43)公開日　平成14年11月８日(2002.11.8)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｓ	２Ｃ００５
Ｂ４２Ｄ　15/10	５０１	Ｂ４２Ｄ　15/10	５０１Ｌ	５Ｂ０５８
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｇ	５Ｂ０８５

審査請求　未請求　請求項の数７　ＯＬ　（全６頁）

(21)出願番号　特願2001－126416(P2001－126416)

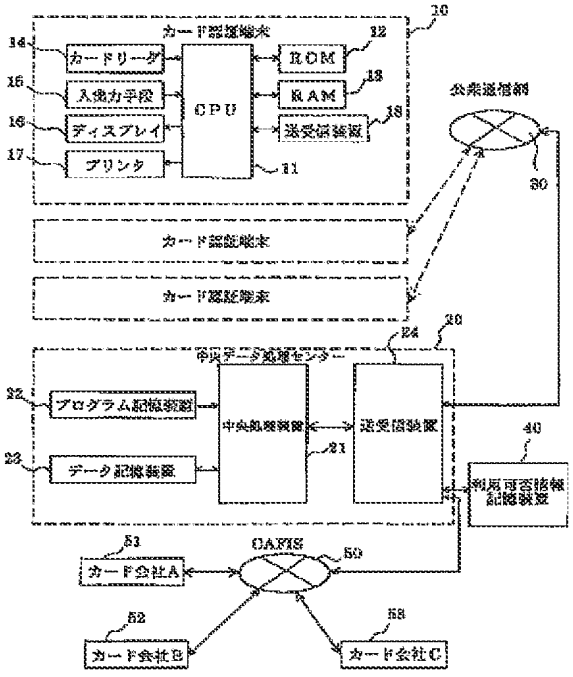
(22)出願日　平成13年４月24日(2001.4.24)

(71)出願人　000002325
セイコーインスツルメンツ株式会社
千葉県千葉市美浜区中瀬１丁目８番地
(72)発明者　立花　仁
千葉県千葉市美浜区中瀬１丁目８番地　セイコーインスツルメンツ株式会社内
(74)代理人　100096378
弁理士　坂上　正明

Ｆターム(参考)　2C005 HA03 HB09 HB20 JB33 LB32 LB36
5B058 CA27 KA02 KA04 KA33 YA02
5B085 AE12 AE23 BA06

(54)【発明の名称】　カード認証システム

(57)【要約】
【課題】　偽造による不正使用を高度に防止できるカード認証システムを提供する。
【解決手段】　多数のカード認証端末１０と、これらカード認証端末と公衆通信網３０を介して接続される中央データ処理センター２０とを具備し、前記中央データ処理センター２０からカードビジネス総合ネットワークシステム５０を介して各カード会社５１～５３のホストコンピュータにオンラインでアクセスすることにより前記カード認証端末１０でオンライン認証処理を行えるようにしたカード認証システムにおいて、各カードの利用者が当該カードの有効無効を事前に切り替えることができる利用可否情報記憶装置４０を有し、前記中央データ処理センター２０は、当該利用可否情報記憶装置４０を介して利用可能と判断したカードに対してのみオンライン認証を行う。



1

【特許請求の範囲】

【請求項１】　多数のカード認証端末と、これらカード認証端末と公衆通信網を介して接続される中央データ処理センターとを具備し、前記中央データ処理センターからカードビジネス総合ネットワークシステムを介して各カード会社のホストコンピュータにオンラインでアクセスすることにより前記カード認証端末でオンライン認証処理を行えるようにしたカード認証システムにおいて、各カードの利用者が当該カードの有効無効を事前に切り替えることができる利用可否情報記憶装置を有し、前記中央データ処理センターは、当該利用可否情報記憶装置を介して利用可能と判断したカードに対してのみオンライン認証を行うことを特徴とするカード認証システム。

【請求項２】　前記利用可否情報記憶装置は、カードの利用者からの利用可変更への要求を受信して当該カードについての利用を有効とすることを特徴とする請求項１に記載のカード認証システム。

【請求項３】　前記利用可否情報記憶装置は、カードの利用者からの利用可変更への要求を受信して当該カードについての利用を有効とした後、所定時間で自動的に利用不可へ変更することを特徴とする請求項２に記載のカード認証システム。

【請求項４】　前記利用可否情報記憶装置は、カードの利用者からの利用可変更への要求を、利用者からの無線通信端末を介して受信することを特徴とする請求項１～３の何れかに記載のカード認証システム。

【請求項５】　前記利用可否情報記憶装置は、カードの利用者からの利用可変更への要求を、利用者からの無線通信端末から前記カード認証端末を経由して受信することを特徴とする請求項１～３の何れかに記載のカード認証システム。

【請求項６】　前記利用可否情報記憶装置は、各カードに付いてのデータを予め有しており、登録されているカードについて利用可否を登録することを特徴とする請求項１～５の何れかに記載のカード認証システム。

【請求項７】　前記利用可否情報記憶装置は、各カードに付いての利用可能となるカードについてのデータのみを随時登録することを特徴とする請求項１～５の何れかに記載のカード認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、クレジットカード又はデビットカードなどの利用者本人が当該カードの利用可否を設定できるようにして、例えば、本人の使用時のみに利用可として不正使用を防止することができるカード認証システムに関する。

【０００２】

【従来の技術】従来のクレジットカードやデビットカードは、カードが発行されると、盗難カード等の利用を無効としたカードや利用限度額を超えたカードなどを除いて、原則的には常に利用可であり、使用時には本人を確認した上で利用可能となる。

【０００３】

【発明が解決しようとする課題】しかしながら、盗難や紛失後、迅速に届け出ができれば問題はないが、届け出が出されるまでには時間がかかることがあり、不正使用が防止できない。また、従来においては、偽造カードによる不正使用に対しては全く無防備である。

【０００４】本発明は、このような事情に鑑み、偽造による不正使用を高度に防止できるカード認証システムを提供することを課題とする。

【０００５】

【課題を解決するための手段】前記課題を解決する本発明の第１の態様は、多数のカード認証端末と、これらカード認証端末と公衆通信網を介して接続される中央データ処理センターとを具備し、前記中央データ処理センターからカードビジネス総合ネットワークシステムを介して各カード会社のホストコンピュータにオンラインでアクセスすることにより前記カード認証端末でオンライン認証処理を行えるようにしたカード認証システムにおいて、各カードの利用者が当該カードの有効無効を事前に切り替えることができる利用可否情報記憶装置を有し、前記中央データ処理センターは、当該利用可否情報記憶装置を介して利用可能と判断したカードに対してのみオンライン認証を行うことを特徴とするカード認証システムにある。

【０００６】本発明の第２の態様は、第１の態様において、前記利用可否情報記憶装置は、カードの利用者からの利用可変更への要求を受信して当該カードについての利用を有効とすることを特徴とするカード認証システムにある。

【０００７】本発明の第３の態様は、第２の態様において、前記利用可否情報記憶装置は、カードの利用者からの利用可変更への要求を受信して当該カードについての利用を有効とした後、所定時間で自動的に利用不可へ変更することを特徴とするカード認証システムにある。

【０００８】本発明の第４の態様は、第１～３の何れかの態様において、前記利用可否情報記憶装置は、カードの利用者からの利用可変更への要求を、利用者からの無線通信端末を介して受信することを特徴とするカード認証システムにある。

【０００９】本発明の第５の態様は、第１～３の何れかの態様において、前記利用可否情報記憶装置は、カードの利用者からの利用可変更への要求を、利用者からの無線通信端末から前記カード認証端末を経由して受信することを特徴とするカード認証システムにある。

【００１０】本発明の第６の態様は、第１～５の何れかの態様において、前記利用可否情報記憶装置は、各カードに付いてのデータを予め有しており、登録されているカードについて利用可否を登録することを特徴とするカ

ード認証システムにある。

【００１１】本発明の第７の態様は、第１～５の何れかの態様において、前記利用可否情報記憶装置は、各カードに付いての利用可能となるカードについてのデータのみを随時登録することを特徴とするカード認証システムにある。

【００１２】かかる本発明によれば、偽造による不正使用を高度に防止できるカード認証システムを提供することができる。

【００１３】

【発明の実施の形態】以下、本発明を一実施形態に基づいて説明する。

【００１４】本発明に係るクレジットカード認証システムの一実施形態の全体概略構成を図１に示す。図１に示すように、多数のカード認証端末１０は、中央データ処理センター２０と、有線又は無線の公衆通信網３０を介して接続されており、中央データ処理センター２０は、専用通信網を介して利用可否情報記憶装置４０と、カードビジネス総合ネットワーク５０とに接続されている。カードビジネス総合ネットワーク５０は、カードエヌ・ティ・ティ・データ通信株式会社のＣＡＦＩＳが代表的なものであり、複数のカード会社５１～５３や金融機関をオンラインで接続するものである。

【００１５】カード認証端末１０は、各種演算と制御を行うＣＰＵ１１と、プログラムが記憶されたＲＯＭ１２と、各種データを記憶するＲＡＭ１３と、要認証クレジットカードの会員情報とカードＩＤとを読みとることができるカードリーダ１４と、料金や支払い方法などの情報を入力するための入出力手段１５と、認証結果等を表示するディスプレイ１６と、利用料金等がプリントアウトされるプリンタ１７と、公衆通信網３０と接続するための送受信装置１８とを主たる構成要素として具備する。

【００１６】中央データ処理センター２０は、各種演算と制御を行う中央処理装置２１と、プログラムが記憶されたプログラム記憶装置２２と、各種データを記憶するデータ記憶装置２３と、公衆通信網３０と接続すると共にカードビジネス総合ネットワークシステム５０と接続するための送受信装置２４とを主たる構成要素として具備する。

【００１７】利用可否情報記憶装置４０は、図２（ａ）に示すように、各種演算と制御を行う中央処理装置４１と、プログラムが記憶されたプログラム記憶装置４２と、各種データを記憶するデータ記憶装置４３と、中央データ処理センター２０と接続するための送受信装置４４と、携帯電話やＰＨＳなどの通信端末６０から直接情報を受信する受理装置４５とを具備し、データ記憶装置４３内には、利用可否情報データベース４６が格納されている。

【００１８】利用可否情報データベース４６は、図２（ｂ）に示すように、例えば、クレジットカードなどのカードを発行する際に、カード番号と共に、利用者がアクセスするための情報、例えば、会員名及びパスワードなどが登録されたデータベースであり、各カードが有効か無効かの情報も具備する。

【００１９】ここで、利用可否情報データベース４６の有効無効の情報は、利用者により随時変更可能となっている。利用者による変更の方法は、特に限定されないが、通信端末を介して接続されるウェブを介して変更できるようにしてもよいし、通信端末６０からのメールを受信することにより変更できるようにしてもよいし、通信端末からの音声指示により変更できるようにしてもよい。

【００２０】また、有効無効の変更は、有効化要求があったら有効、無効化要求があったら無効とするようにしてもよいが、原則的には無効としておき、有効化要求があった後、所定時間のみ、例えば、２，３分、５分、１０分などの短時間、又は１日などの所定時間だけ、有効化した後、自動的に無効化するようにするのが好ましい。これは、利用者が利用する際だけ有効化しておくことにより、偽造カードの不正使用を未然に防止するためである。

【００２１】なお、受理装置４５は、正規の利用者からの有効化要求のみを受理し、不正使用者からの不正な要求を受理しないように、アクセスするのに所定のパスワードを要求するようにするのが好ましく、また、通信端末の発信者通知をパスワードとするようにしてもよい。

【００２２】このような不正利用を防止しつつ利用者が容易に有効化要求を行えるようにするためには、例えば、カード番号と予め登録したパスワード及び所定の会員情報及び有効化要求と共に通信端末のメール機能で送信するようにしてもよい。また、通信端末に所定の暗号化処理（一方向演算）を行えるようなアプリケーションを格納しておき、カードの会員番号と予め登録した暗号化鍵とを用いて所定の暗号化処理した結果をパスワードとし、これを所定の会員情報及び有効化要求と共にメール機能を用いて送信するようにしてもよい。

【００２３】また、利用可否情報データベース４６には、有効なカードのみの番号を存在させるようにしてもよい。すなわち、受理装置４５は、有効化要求と共に受理したカード番号のみを利用可否情報データベース４６に登録し、利用可否情報データベース４６にカード番号が存在する場合にはカードが有効であるとする。なお、この場合、不正使用者からのアクセスを防止するため、カード発行時に所定の暗号化処理を行ったときに所定の結果になるようなパスワード、例えば、所定の計算を行うと結果は常に零となるようなパスワードを発行し、このようなパスワードと共に送信されたカード番号のみを登録するようにして、不正登録を排除する必要がある。

【００２４】以上説明したカード認証システムにおい

て、カードを利用する場合には、利用者は、予め、好ましくは利用直前に、携帯電話等の通信端末を介して利用可否情報記憶装置４０の受理装置４５へ有効化要求を送信しておく必要がある。その後、その利用者は、店舗やサービスカウンターに設置されたカード認証端末１０で、利用可能か否かのチェックを受ける。すなわち、図３に示すように、カード認証端末１０は、カードリーダ１４で会員情報及びカード番号を読みとる（ステップＳ１１）。これを送受信装置１８から公衆通信網３０を介して中央データ処理センター２０へ送信する（ステップＳ１２）。中央データ処理センター２０は、要認証のカード情報を受信すると、当該カードの利用可否を利用可否情報記憶装置４０へ問い合わせ、利用可否判定結果の受信を待つ（ステップＳ１３）。利用可否判定結果から当該カードの利用の可否を判断し（ステップＳ１４）、利用不可の場合には（ステップＳ１４、Ｎｏ）、利用不可をカード認証端末へ利用不可と判定する（ステップＳ１５）。

【００２５】一方、利用可能だった場合には（ステップＳ１４、Ｙｅｓ）、受信した要認証カードの会員情報及びカード番号から会員情報を分離し、これを所定のフォーマット化データに変換し、カードビジネス総合ネットワークシステム５０を介して特定のカード会社へ送信し（ステップＳ１６）、カード会社からの認証結果を待つ（ステップＳ１７）。

【００２６】カード会社からの認証結果を受信すると、要認証カードが無効カードか否かを判断し（ステップＳ１８）、無効カードと判断した場合には（ステップＳ１８、Ｙｅｓ）利用不可と判定し（ステップＳ１５）、無効カードでないと判断したときに（ステップＳ１８、Ｎｏ）は、有効と判断し（ステップＳ１９）、認証する旨の情報をカード認証端末１０へ送信する（ステップＳ２０）。なお、利用金額や支払い方法等のデータを処理は通常のクレジットカードやデビットカードの処理と同一であるので、説明は省略する。

【００２７】以上説明した実施形態によると、利用者がカード利用時のみにカード利用を有効としておくことができるので、偽造カード等によるカードの不正使用を防止することができる。

【００２８】なお、以上説明した実施形態では、利用者がカードの利用可否の変更の要求をする場合、通信端末６０から利用可否情報記憶装置４０へ直接送信するようにしたが、カード認証端末１０へ送信するようにし、カード認証端末１０から中央データ処理センター２０を介して利用可否情報記憶装置４０へ送信されるようにしてもよい。この場合、通信端末６０とカード通信端末１０とは、例えば、Bluetoothなどの無線規格により、例えば自動的に接続して通信できるようにしてもよい。

【００２９】また、上述した実施形態では、利用可否情報記憶装置４０は中央データ処理センター２０とは別途設置するようにしたが、中央データ処理センター２０内に設置してもよいことは言うまでもない。

【００３０】

【発明の効果】以上説明したように、本発明によれば、偽造による不正使用を高度に防止できるカード認証システムを提供することができるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るカード認証システムの概略構成を示す図である。

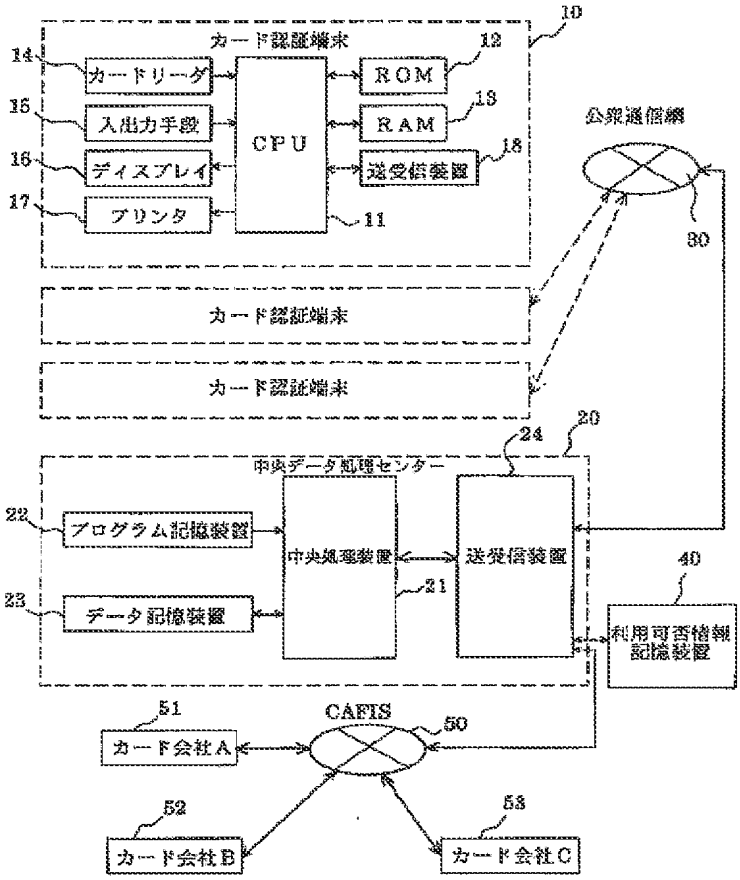
【図２】本発明の利用可否情報記憶装置の概略を示す図である。

【図３】本発明の一実施形態に係るカード認証システムの認証の手順を示す図である。

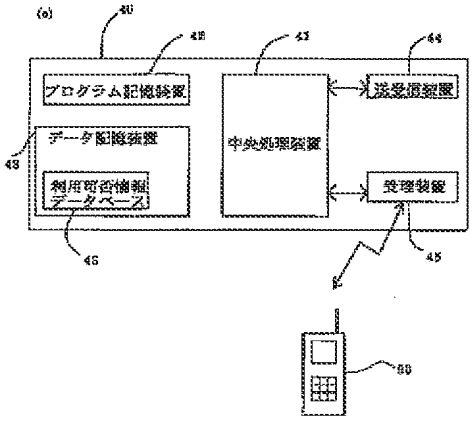
【符号の説明】

１０　カード認証端末
２０　中央データ処理センター
３０　公衆通信網
４０　利用可否情報記憶装置
５０　ＣＡＦＩＳ

【図１】



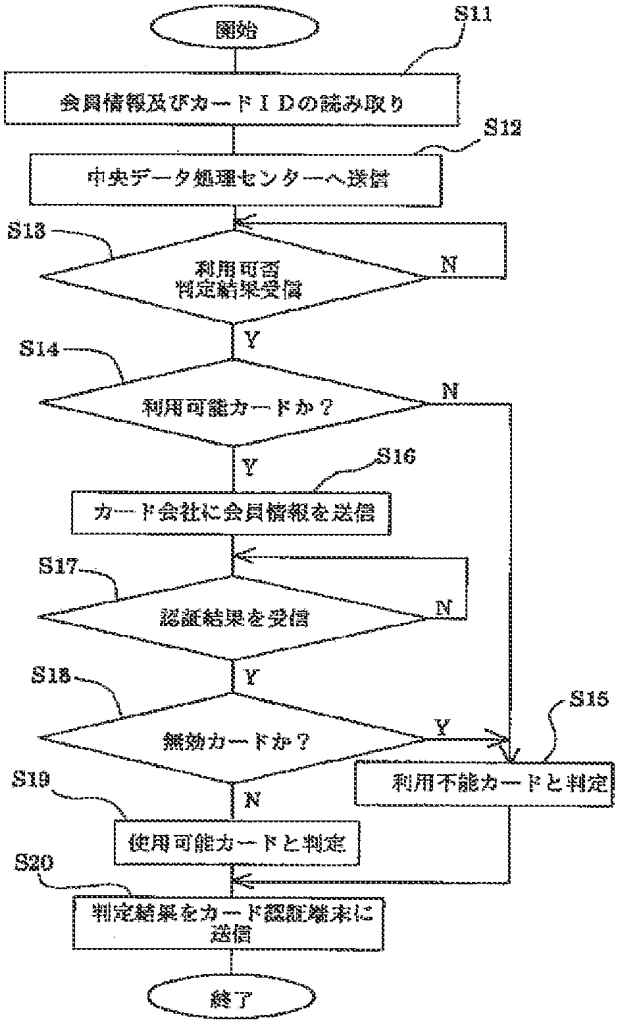
【図２】



(b)　47

No	カード番号	有効	無効
1	1234567890	✓	
2	0876543210		✓
3	1111222333		✓
4	4444555666	✓	
⋮			

【図３】


開始
S11
会員情報及びカードＩＤの読み取り
S12
中央データ処理センターへ送信
S13
利用可否
判定結果受信
N
Y
S14
利用可能カードか？
N
Y
S16
カード会社に会員情報を送信
S17
認証結果を受信
N
Y
S18
無効カードか？
Y
S15
利用不能カードと判定
N
S19
使用可能カードと判定
S20
判定結果をカード認証端末に
送信
終了

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成20年1月10日(2008.1.10)

【公開番号】特開2002-324219(P2002-324219A)
【公開日】平成14年11月8日(2002.11.8)
【出願番号】特願2001-126416(P2001-126416)
【国際特許分類】
　Ｇ０６Ｋ　17/00　(2006.01)
　Ｂ４２Ｄ　15/10　(2006.01)
　Ｇ０６Ｆ　21/20　(2006.01)
【ＦＩ】
　Ｇ０６Ｋ　17/00　S
　Ｂ４２Ｄ　15/10　５０１Ｌ
　Ｇ０６Ｆ　15/00　３３０Ｇ

【手続補正書】
【提出日】平成19年11月19日(2007.11.19)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】　複数のカード認証端末と、該複数のカード認証端末と公衆通信網を介して接続される中央データ処理センターとを具備し、前記中央データ処理センターからカードビジネス総合ネットワークシステムを介して各カード会社のホストコンピュータにオンラインでアクセスすることにより前記カード認証端末でオンライン認証処理を行うカード認証システムにおいて、
各カードの利用者が当該カードの有効無効を事前に切り替えることができる利用可否情報記憶装置を有し、前記中央データ処理センターは、当該利用可否情報記憶装置を介して利用可能と判断したカードに対してのみオンライン認証を行うことを特徴とするカード認証システム。
【請求項２】　前記利用可否情報記憶装置は、カードの利用者からの利用可変更への要求を受信して当該カードについての利用を有効とすることを特徴とする請求項１に記載のカード認証システム。
【請求項３】　前記利用可否情報記憶装置は、カードの利用者からの利用可変更への要求を受信して当該カードについての利用を有効とした後、所定時間で自動的に利用不可へ変更することを特徴とする請求項２に記載のカード認証システム。
【請求項４】　前記利用可否情報記憶装置は、カードの利用者からの利用可変更への要求を、利用者からの無線通信端末を介して受信することを特徴とする請求項１～３の何れかに記載のカード認証システム。
【請求項５】　前記利用可否情報記憶装置は、カードの利用者からの利用可変更への要求を、利用者からの無線通信端末から前記カード認証端末を経由して受信することを特徴とする請求項１～３の何れかに記載のカード認証システム。
【請求項６】　前記利用可否情報記憶装置は、各カードに付いてのデータを予め有しており、登録されているカードについて利用可否を登録することを特徴とする請求項１～５の何れかに記載のカード認証システム。
【請求項７】　前記利用可否情報記憶装置は、各カードに付いての利用可能となるカードについてのデータのみを随時登録することを特徴とする請求項１～５の何れかに記載

のカード認証システム。